



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/082,235	02/26/2002	John B. Beavers	SYMC1024	3484
34350	7590	02/21/2006		
GUNNISON, MCKAY & HODGSON, L.L.P. 1900 GARDEN ROAD, SUITE 220 MONTEREY, CA 93940				
			EXAMINER	
			PERUNGAVOOR, VENKATANARAY	
			ART UNIT	PAPER NUMBER
			2132	

DATE MAILED: 02/21/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

10/082,235

Applicant(s)

BEAVERS, JOHN B.

Examiner

Venkatanarayanan Perungavoor

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
 - If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
 - Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 31 January 2006.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1,2,4-10 and 12-26 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1,2,4-10 and 12-26 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

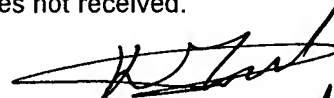
Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 26 February 2002 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.


Kambiz Zand

Attachment(s)

- | | |
|---|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Response to Arguments

1. Applicant's arguments filed 1/31/2006 have been fully considered but they are not persuasive. As U.S. Patent 6,208,720 B1 to Curtis et al.(hereinafter Curtis) discloses the displaying of incident ticket see Col 11 Ln 20-31, tracking rules that are editable by the user viewing the ticket see Col 3 Ln 19-22 & Col 11 Ln 50-59 & Col 2 Ln 50-59.
2. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Response to Amendment

Claim Rejections - 35 USC § 102

3. Claim 1-2,4-10,12-26 are rejected under 35 U.S.C. 102(a) as being anticipated by U.S. Patent 6208720 B1 to Curtis et al.(hereinafter Curtis).
4. Regarding Claim 1, Curtis discloses the providing a number of alert indications containing information related to the incident see Fig. 4 item 408; comparing one or more alert indications to a set of rules and declaring a incident if a match is found see Fig. 4 item 424; comparing one or more alert indications to a decision table and remembering alert indication and comparing to a correlation data see Fig. 2 item 214-220; declaring an incident based on threshold value see Fig. 4 item 414-416; and the displaying of incident ticket including a description of

incident, a conclusion based on the ticket, any actions responsive to the conclusion, one or more user editable incident tracking rules which identify the alert indications for association with the incident and detail of the alert indications see Fig. 5C item 532, 534, 536 & Col 5 Ln 31-64. And also see arguments above.

5. Regarding Claim 2, Curtis discloses the defined default threshold value is level of severity in alert indications see Col 18 Ln 35-44.
6. Regarding Claim 4, Curtis discloses tracking further based on alert indications and associating user editable tracking rules along with it see Col 22 Ln 65- Col 23 Ln 21 & Col 22 Ln 3-11.
7. Regarding Claim 5, Curtis discloses the associating step being performed after passing threshold value and table containing categories and alert codes see Col 18 Ln 13-29.
8. Regarding Claim 6, 21, Curtis discloses the updating of user editable tracking rules see Col 19 Ln 23-40.
9. Regarding Claim 7, Curtis discloses the normalizing of alert information see Fig. 1 item 124.

10. Regarding Claim 8, 16, 20 Curtis discloses the plurality of devices supplying the alert indications see Col 7 Ln 1-20 & Fig. 3 item 152a-n.

11. Regarding Claim 9, Curtis discloses the default value being derived from a set of rules see Col 13 Ln 43-55.

12. Regarding Claim 10, Curtis discloses the a decision table and set of correlation data that identifies patterns and declaring a incident if a match occurs see Col 10 Ln 24-30 & Col 9 Ln 45-53; a set of rules containing a number of queries and matching rules and inputted alert indications see Col 11 Ln 20-49; set of default standards specifying minimum value declare an incident see Col 18 Ln 44-59 and the displaying of incident ticket including a description of incident, a conclusion based on the ticket, any actions responsive to the conclusion, one or more user editable incident tracking rules which identify the alert indications for association with the tickey and detail of the alert indications see Fig. 5C item 532, 534, 536 & Col 5 Ln 31-64. And also see arguments above.

13. Regarding Claim 12, 19 Curtis discloses the filtering out inputted indication that don't meet threshold value and comparing information to rules see Col 18 Ln 13-35.

14. Regarding Claim 13-14, Curtis discloses the database storing declared incidents see Fig. 1 item 130.

15. Regarding Claim 15, Curtis discloses the linking users via global network see Fig. 1 item 102, 104, 106.

16. Regarding Claim 16, Curtis discloses the displaying of incidents see Col 11 Ln 39-49 & Fig. 3 item 152a-n.

17. Regarding Claim 17, Curtis discloses the combination of customized and default rules see Col 3 Ln 6-23.

18. Regarding Claim 22, Curtis discloses the updating through human based observations see Col 11 Ln 31-38.

19. Regarding Claim 23, Curtis discloses the providing a number of alert indications containing information related to the incident see Fig. 4 item 408; comparing one or more alert indications to a set of rules and declaring a incident if a match is found see Fig. 4 item 424; comparing one or more alert indications to a decision table and remembering alert indication and comparing to a correlation data see Fig. 2 item 214-220; declaring an incident based on threshold value see Fig. 4 item 414-416; and the displaying of incident ticket including a description of

incident, a conclusion based on the ticket, any actions responsive to the conclusion, one or more user editable incident tracking rules which identify the alert indications for association with the incident and detail of the alert indications see Fig. 5C item 532, 534, 536 & Col 5 Ln 31-64; a user uses an menu to change/update the alert indications see Col 28 Ln 26-33 & Col 15 Ln 29-36. And also see arguments above.

20. Regarding Claim 24, Curtis discloses the rules includes a source IP address, at least one target address, a conjunction, an attribute name, a condition and an attribute value see Fig. 5C item 532,534,536 & Col 9 Ln 46-60 & Col 25 Ln 34-40 & Col 23 Ln 22-31 & Col 22 Ln 3-11.

21. Regarding Claim 25, Curtis discloses information relating to unauthorized access attempt see Col 5 Ln 44-59 & Col 20 Ln 39-46.

22. Regarding Claim 26, Curtis discloses the alert indications relating to port scans see Col 15 Ln 20-25 & Fig. 1 item 101, 107 & Col 9 Ln 40-45.

Conclusion

23. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a). A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this

action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

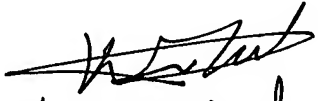
24. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Venkatanarayanan Perungavoor whose telephone number is 571-272-7213. The examiner can normally be reached on 8-4:30. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2132

25. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Venkatanarayanan Perungavoor
Examiner
Art Unit 2132

VP
2/14/2006


Kambiz Zand
Primary Examiner AU 2132